奇怪的文件

发表于 2021-01-25 更新于 2021-06-16 分类于 Challenge， 2019， 工业信息安全技能大赛， 山东站
Challenge | 2019 | 工业信息安全技能大赛 | 山东站 | 奇怪的文件

点击此处获得更好的阅读体验

WriteUp来源

来自MO1N战队

题目描述

> *在上位机中发现奇怪的文件，你能发现其中的秘密吗？flag形式为flag{}*

题目考点

- *ZIP文件格式*
- *ZIP密码爆破*
- *pyc反编译*
- *LSB加密隐写*

解题思路

附件为3个part。查看头似乎为zip压缩包。

首先给每个part添加504b之后拼接到一起得到加密的zip压缩包，但是压缩包显然是有问题的

把压缩包拖入010editor

对照part1和part2之后发现。part1缺少了CRC校验数据，part2缺少了文件名

将缺失的数据补齐之后，就可以获得正常的压缩包了，正常的压缩包MD5应当为6c925e9ba10d9ba5b46c87db41c61106

然后使用大写小写数字爆破zip密码。爆破出来密码为GyxXaq9

之后解压得到一张图片，在图片尾部发现一段数据

把这段数据单独拉出来，翻到末尾看起来像是一个倒序的zip文件（倒着查看为504b0304）

写程序恢复为正常的文件

```
#!/usr/bin/env python3
# 读文件
with open("111", "rb") as f:
    data = f.read()

# 写文件
with open("new_data.zip", "wb") as f:
    f.write(data[::-1])
```

之后打开新的zip文件

是一个pyc，直接解压后在线反编译即可，反编译出的代码如下

```
#!/usr/bin/env python
# visit http://tool.lu/pyc/ for more information
import random
import base64
import sys

def KeyGenerate():
    random.seed(10)
    keyseed = ''
    for i in range(12):
        x = random.randint(32, 127)
        keyseed += chr(x)

    return base64.b64encode(keyseed.encode('utf-8')).decode('utf-8')


def enc(key, file):
    count = 0
    f = open(file, 'rb')
    f1 = open('encrypted', 'wb')
    for now in f:
        for nowByte in now:
            newByte = nowByte ^ ord(key[count % len(key)])
            count += 1
            f1.write(bytes([
                newByte]))


if __name__ == '__main__':
    key = KeyGenerate()
    enc(key, sys.argv[1])
```

因为key生成函数中定义了种子始终为10，所以加解密使用的key都一样，为aSRWXWkhOlteQ3M0

查看算法为异或，即加解密使用的算法应当一样，直接再次调用加密函数即可解密

```
#!/usr/bin/env python
import random
import base64

def KeyGenerate():
    random.seed(10)
    keyseed = ''
    for i in range(12):
        x = random.randint(32, 127)
        keyseed += chr(x)
    return base64.b64encode(keyseed.encode('utf-8')).decode('utf-8')

def dec(key):
    f = open('encrypted', 'rb')
    f1 = open('decrypted', 'wb')
    for now in f:
        for nowByte in now:
            newByte = nowByte ^ ord(key[count % len(key)])
            count += 1
            f1.write(bytes([newByte]))

if __name__ == '__main__':
    key = KeyGenerate()
    dec(key)
```

解密出的文件为一个png图片

该图片有LSB隐写，但隐写信息加密

使用https://github.com/livz/cloacked-pixel中的工具对隐写密码爆破。最终爆破出的密码为U!lSb29

从decrypted.png中释放出来一个jpg文件，打开文件发现是一半flag

使用字体宋体，字号大约20左右，肉眼识别获得完整flag

Flag

```
flag{2ceuagIha7v8mlfod9uas1d86wqer0}
```

- **本文作者：** CTFHub
- **本文链接：** https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/山东站/o34Q8Erf8Uh1ahBvHtPMYq.html
- **版权声明：** 本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！

Challenge # 2019 # 工业信息安全技能大赛 # 山东站
简单流量分析
简单的工控固件逆向